CHAPTER 5

Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping.

This chapter includes the following topics:

Information about IGMP Snooping

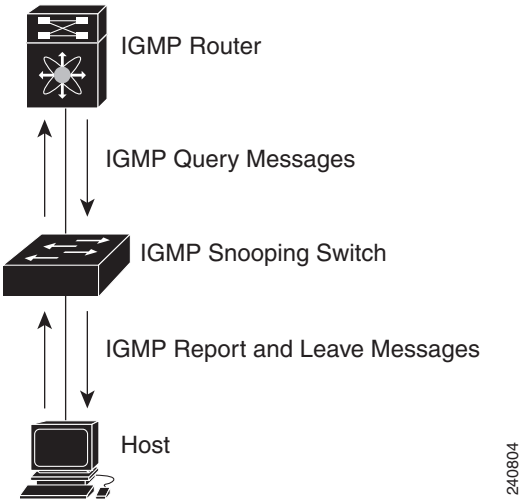
This section includes the following topics:

Introduction

The Internet Group Management Protocol (IGMP) snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the device.

Figure 5-1 shows an IGMP snooping switch that sits between the host and the IGMP router. The IGMP snooping switch snoops the IGMP membership reports and Leave messages and forwards them only when necessary to the connected IGMP routers.

Figure 5-1 IGMP Snooping Switch



The IGMP snooping software operates upon IGMPv1, IGMPv2, and IGMPv3 control plane packets where Layer 3 control plane packets are intercepted and influence the Layer 2 forwarding behavior.

The Cisco Nexus 1000V IGMP snooping implementation has the following proprietary features:

- Multicast forwarding based on IP address rather than MAC address.
- Optimized multicast flooding (OMF) that forwards unknown traffic to routers only and performs no data driven state creation.

For more information about IGMP snooping, see RFC 4541.

IGMPv1 and IGMPv2

If no more than one host is attached to each VLAN switch port, then you can configure the fast leave feature in IGMPv2. The fast leave feature does not send last member query messages to hosts. As soon as the software receives an IGMP leave message, the software stops forwarding multicast data to that port.

IGMPv1 does not provide an explicit IGMP leave message, so the software must rely on the membership message time-out to indicate that no hosts remain that want to receive multicast data for a particular group.

Report suppression is not supported and is disabled by default.

Note The software ignores the configuration of the last member query interval when you enable the fast leave feature because it does not check for remaining hosts.

IGMPv3

IGMPv3 snooping provides constrained flooding based on the group IP information in the IGMPv3 reports.

By default, the software tracks hosts on each VLAN port. The explicit tracking feature provides a fast leave mechanism. Because every IGMPv3 host sends membership reports, report suppression limits the amount of traffic that the switch sends to other multicast capable routers.

Even though the IGMPv3 membership reports provide a full accounting of group members on a LAN segment, when the last host leaves, the querier sends a membership query. You can configure the parameter last member query interval. If no host responds before the time-out, the software removes the group state. If the querier specifies a mean-response-time (MRT) value in the queries, it overrides the last member query interval configuration.

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged in to the switch.
- A querier must be running on the uplink switches on the VLANs that contain multicast sources and receivers.

  When the multicast traffic does not need to be routed, you must configure an external switch to query membership. On the external switch, define the query feature in a VLAN that contains multicast sources and receivers but no other active query feature. In Cisco Nexus 1000V, report suppression is not supported and is disabled by default.

  When an IGMP snooping query feature is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts wanting to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to identify accurate forwarding.

Default Settings

Table 5-1 lists the default settings for IGMP snooping parameters.

Table 5-1 Default IGMP Snooping Parameters

Parameters	Default
IGMP snooping	Enabled
IGMPv3 Explicit tracking	Enabled
IGMPv2 Fast leave	Disabled
Last member query interval	1 second
Link-local groups suppression	Enabled
Snooping querier	Disabled
IGMPv1/v2 Report suppression	Disabled
IGMPv3 Report suppression	Disabled

Enabling or Disabling IGMP Snooping Globally for the VSM

You can use this procedure to enable or disable IGMP snooping globally for the VSM.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- IGMP snooping is enabled globally on the VSM (the default). If enabled globally, you can turn it on or off per VLAN.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip igmp snooping**
3. **show ip igmp snooping** [**vlan** *vlan-id*]
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ip igmp snooping**
	
	Example:
	`n1000v(config)# no ip igmp snooping`
	`n1000v(config)#`
		Enables or disables IGMP snooping in the running configuration for all VLANs. The default is enabled. If you have previously disabled the feature then you can enable it with this command.
		
		Note If disabled, then IGMP snooping on all VLANs is disabled.

	Command	Purpose
Step 3	**show ip igmp snooping** [**vlan** *vlan-id*] **Example:** n1000v(config)# show ip igmp snooping n1000v(config-vlan)# show ip igmp snooping Global IGMP Snooping Information: IGMP Snooping enabled IGMPv1/v2 Report Suppression disabled IGMPv3 Report Suppression disabled Link Local Groups Suppression enabled IGMP Snooping information for vlan 1 IGMP snooping enabled IGMP querier none Switch-querier disabled IGMPv3 Explicit tracking enabled IGMPv2 Fast leave disabled IGMPv1/v2 Report suppression disabled IGMPv3 Report suppression disabled Link Local Groups suppression enabled Router port detection using PIM Hellos, IGMP Queries Number of router-ports: 0 Number of groups: 0 Active ports: --More-- n1000v(config)#	(Optional) Displays the configuration for verification
Step 4	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring IGMP Snooping on a VLAN

You can use this procedure to configure IGMP snooping on a VLAN.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- IGMP snooping is enabled by default for all VLANs in the VSM.

Note If IGMP snooping is disabled globally, it takes precedence over the VLAN state.

- Table 5-2 lists and describes the parameters available for configuring IGMP snooping on a VLAN.

Table 5-2 IGMP Snooping Parameters

Parameter	Description
IGMP snooping	Enables IGMP snooping per VLAN. **Note** IGMP snooping must be enabled globally (the default) in order to toggle it on or off per VLAN. If IGMP snooping is disabled globally, then it cannot be enabled per VLAN.
Explicit tracking	Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis. The default is enabled.
Fast leave	Enables the software to remove the group state when it receives an IGMP Leave report without sending an IGMP query message. This parameter is used for IGMPv2 hosts when no more than one host is present on each VLAN port. The default is disabled.
Last member query interval	Sets the interval the software waits after sending an IGMP query to verify that no hosts that want to receive a particular multicast group remain on a network segment. If no hosts respond before the last member query interval expires, the software removes the group from the associated VLAN port. Values range from 1 to 25 seconds. The default is 1 second.
Link-local groups suppression	Configures link-local groups suppression. The default is enabled. **Note** You can also enable link-local suppression globally on all interfaces in the VSM by entering the **ip igmp snooping link-local-groups-suppression** command from global configuration mode.
Multicast router	Configures a static connection to a multicast router. The interface to the router must be in the selected VLAN.
Static group	Configures a Layer 2 port of a VLAN as a static member of a multicast group.

SUMMARY STEPS

1. **config t**
2. **vlan** *vlan-id*
3. **ip igmp snooping**
4. (Optional) **ip igmp snooping explicit-tracking**
5. (Optional) **ip igmp snooping fast-leave**
6. (Optional) **ip igmp snooping last-member-query-interval** *seconds*
7. (Optional) **ip igmp snooping mrouter interface type** *if_id*
8. (Optional) **ip igmp snooping static-group** *group-ip-addr* **interface type** *if_id*
9. (Optional) **ip igmp snooping link-local-groups-suppression**

10. **show ip igmp snooping** [**vlan** *vlan-id*]
11. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**vlan** *vlan-id*
	
	Example:
	`n1000v(config)# vlan 2`
	`n1000v(config-vlan)#`
		Enters configuration mode for the specified VLAN.

Step 3	[**no**] **ip igmp snooping** **Example:** `n1000v(config-vlan)# ip igmp snooping`	(Optional) Enables or disables IGMP snooping in the running configuration for the specific VLAN. If IGMP snooping is enabled for the VSM, then IGMP snooping is enabled for the VLAN by default.

Step 4	[**no**] **ip igmp snooping explicit-tracking**
	
	Example:
	`n1000v(config-vlan)# ip igmp snooping explicit-tracking`
	`n1000v(config-vlan)#`
		(Optional) Tracks IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis in the running configuration.
		The default is enabled.

Step 5	[**no**] **ip igmp snooping fast-leave**
	
	Example:
	`n1000v(config-vlan)# ip igmp snooping fast-leave`
	`n1000v(config-vlan)#`
		(Optional) Enables fast-leave for the specified VLAN in the running configuration.
		Fast-leave supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol.
		When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port.
		The default is disabled.

Step 6	[**no**] **ip igmp snooping last-member-query-interval** *seconds*
	
	Example:
	`n1000v(config-vlan)# ip igmp snooping last-member-query-interval 3`
	`n1000v(config-vlan)#`
		(Optional) Establishes a time interval in seconds after which the group is removed from the associated VLAN port if no hosts respond to an IGMP query message. This interval is saved in the running configuration
		Allowable intervals are from 1 (default) to 25 seconds.

Step 7	[**no**] **ip igmp snooping mrouter interface** *interface*
	
	Example:
	`n1000v(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1`
	`n1000v(config-vlan)#`
		(Optional) Configures a static connection for the VLAN to a multicast router in the running configuration.
		The interface to the router must be in the specified VLAN. You can specify the interface by the type and the number, such as **ethernet** *slot/port*.
		vEths are not supported as router ports.

	Command	Purpose

Step 8	**[no] ip igmp snooping static-group** *group-ip-addr* **interface type** *if_id*
	
	Example:
	`n1000v(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`
	`n1000v(config-vlan)#`
		(Optional) Configures a VLAN Layer 2 port as a static member of a multicast group in the running configuration.
		
		You can specify the interface by the type and the number, such as **ethernet** *slot/port*.

Step 9	**[no] ip igmp snooping link-local-groups-suppression**
	
	Example:
	`n1000v(config-vlan)# ip igmp snooping link-local-groups-suppression`
	`n1000v(config-vlan)#`
		(Optional) Configures link-local groups suppression. The default is enabled.
		
		Note You can apply link-local groups suppression to all interfaces in the VSM by entering this command in global configuration mode.

Step 10	**show ip igmp snooping** [**vlan** *vlan-id*]
	
	Example:
	`n1000v(config-vlan)# show ip igmp snooping vlan 2`
	`IGMP Snooping information for vlan 5`
	`  IGMP snooping enabled`
	`  IGMP querier none`
	`  Switch-querier disabled`
	`  IGMPv3 Explicit tracking enabled`
	`  IGMPv2 Fast leave enabled`
	`  IGMPv1/v2 Report suppression disabled`
	`  IGMPv3 Report suppression disabled`
	`  Link Local Groups suppression enabled`
	`  Router port detection using PIM Hellos, IGMP Queries`
	`  Number of router-ports: 0`
	`  Number of groups: 0`
	`  Active ports:`
	`n1000v(config)#`
		(Optional) Displays the configuration for verification

Step 11	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the IGMP Snooping Configuration

Use the following commands to display the IGMP snooping configuration information.

Command	Purpose
show ip igmp snooping [**vlan** *vlan-id*]	Displays IGMP snooping configuration by VLAN.
show ip igmp snooping groups [**vlan** *vlan-id*] [**detail**]	Displays IGMP snooping information about groups by VLAN.
show ip igmp snooping querier [**vlan** *vlan-id*]	Displays IGMP snooping queriers by VLAN.

Command	Purpose
show ip igmp snooping mroute [**vlan** *vlan-id*]	Displays multicast router ports by VLAN.
show ip igmp snooping explicit-tracking [**vlan** *vlan-id*]	Displays IGMP snooping explicit tracking information by VLAN.

For detailed information about commands and their output, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

Example Configuration for IGMP Snooping

This example shows how to enable IP IGMP snooping for the VSM, and make the following optional configurations for VLAN 2:

- Tracking of IGMPv3 membership reports from individual hosts for each port.
- A static connection to a multicast router through Ethernet 2/1.
- Static membership in multicast group 230.0.0.1.

```
config t
ip igmp snooping
vlan 2
ip igmp snooping
ip igmp snooping explicit-tracking
ip igmp snooping mrouter interface ethernet 2/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
show ip igmp snooping vlan 2
copy run start
```

Additional References

For additional information related to implementing IGMP snooping, see the following sections:

- Related Documents, page 5-9
- Standards, page 5-10

Related Documents

Related Topic	Document Title
Port Profiles	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*
Interfaces	*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IGMP Snooping

This section provides the release history for the IGMP snooping feature.

Table 5-3

Feature Name	Releases	Feature Information
Link-local suppression	4.2(1)SV1(4)	Added support to enable or disable link-local group suppression.
Report suppression	4.0(4)SV1(3)	Removed support for report suppression.
IGMP Snooping	4.0(4)SV1(1)	This feature was introduced.